

UNITED STATES DISTRICT COURT
for the
Eastern District of Pennsylvania

In the Matter of the Search of _____
(Briefly describe the property to be searched
or identify the person by name and address) _____)
One Samsung cellular telephone model SM- G935A _____)
bearing serial no. RF8HB3BTYND located at the _____)
Lancaster PD Station, 39 West Chester St, Lancaster, PA _____)
Case No. 19- 1902 -M

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A.

located in the Eastern District of Pennsylvania, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

evidence of a crime;
 contraband, fruits of crime, or other items illegally possessed;
 property designed for use, intended for use, or used in committing a crime;
 a person to be arrested or a person who is unlawfully restrained.

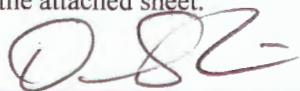
The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. Section 2422(b)	Knowing use of an interstate commerce facility to entice a minor to engage in sexually explicit conduct.
18 U.S.C. Section 2423(b)	Travel with the intent to engage in illicit sexual conduct.

The application is based on these facts:

See attached affidavit.

Continued on the attached sheet.
 Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

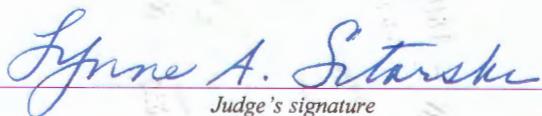
FBI Special Agent, DARON SCHREIER

Printed name and title

Sworn to before me and signed in my presence.

Date: Nov. 12, 2019

City and state: Philadelphia, PA



Judge's signature

LYNNE A. SITARSKI U.S. Chief Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF:
SAMSUNG CELLULAR PHONE MODEL
SM-G935A BEARING SERIAL NUMBER
RF8HB3BTYND, CURRENTLY LOCATED
AT THE LANCASTER POLICE STATION
39 WEST CHESTER STREET LANCASTER,
PENNSYLVANIA

Case No. 19-1902-M

AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE

I, Daron Schreier, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the seizure and examination of property—an electronic device—currently in possession of law enforcement, and the extraction from that property of electronically stored information described in Attachment B.

2. I have been employed as a Special Agent for the Federal Bureau of Investigation (“FBI”) for 13 years, and am currently assigned to the Philadelphia Division’s Violent Crimes Against Children Squad. While employed by the FBI, I have investigated federal criminal violations related to counterterrorism, counterintelligence, cybercrime, child pornography, and child sexual exploitation. I have gained experience through training at the FBI Academy, training at FBIHQ, various conferences, and everyday work related to conducting these types of investigations. Because I am a government agent engaged in enforcing the criminal laws, and am

authorized by the Attorney General to request a search warrant, I am a “federal law enforcement officer” as defined by Fed. R. Crim. P. 41(a)(2)(C).

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts contained in this affidavit are derived from my own investigation as well as from other law enforcement officers and witnesses.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. This application seeks authorization to search a Samsung cellular telephone, Model SM-G935A bearing serial number RF8HB3BTYND, hereinafter the “SUBJECT PROPERTY,” further described in Attachment A, and currently secured and located at the Lancaster Police Station located at 39 West Chestnut Street, Lancaster, Pennsylvania, to search for, evidence, contraband, fruits and instrumentalities of violations of 18 U.S.C. § 2422 (b) and 2423(b), use of an interstate commerce facility to entice a minor to engage in sexually explicit conduct and travel with intent to engage in illicit sexual conduct, in the form of electronically stored data further described in Attachment B.

5. 18 U.S.C. § 2422(b) makes it a crime to knowingly use a facility and means of interstate and foreign commerce to persuade, induce , entice and coerce a person who had not attained the age of 18 years to engage in sexual activity for which any person could be charged with a criminal offense.

6. 18 U.S.C. § 2423(b) makes it a crime to travel in interstate commerce for the purpose of engaging in illicit sexual conduct with a person who had not attained the age of 18.

PROBABLE CAUSE

7. On January 17, 2019, Joseph Bleier, a/k/a "Mike," a/k/a "polar bear," was indicted by a federal grand jury in the Eastern District of Pennsylvania in a two-count indictment and charged in Count One with using a facility and means of interstate commerce, that is, the Internet, to persuade, induce, entice and coerce Minor #1, who had not attained the age of 18 years, to engage in sexual activity for which any person could be charged with a criminal offense, that is defendant Joseph Bleier enticed and attempted to entice Minor #1 to engage in involuntary deviate sexual conduct, in violation of 18 Pa.C.S. § 3123, and aggravated indecent assault of a person under the age of 16 years, in violation of 18 Pa.C.S. § 3125(a)(8). Bleier was also charged in Count Two with traveling in interstate commerce from the State of New York to Lancaster, Pennsylvania for the purpose of engaging in illicit sexual conduct with Minor #1, a person who had not attained the age of 18.

8. Minor #1, named in the indictment, advised law enforcement that from May 2016 to August 2016, she engaged in an online relationship with an individual later identified to be Joseph BLEIER. Minor #1 advised law enforcement that she and BLEIER had discussions that were sexual in nature as well as exchanged photographs of each other's genitalia. Minor #1 advised she sent photographs of her vagina and breasts to BLEIER at his request. Minor #1 advised she and BLEIER used the following online platforms to communicate: Meow Chat, KIK, Instagram, and Skype.

9. Minor #1 also advised law enforcement she and BLEIER used multiple online social network sites to arrange a time and date for BLEIER to travel to Lancaster, Pennsylvania for the purpose of engaging in sexual conduct. Minor #1 advised that she and BLEIER did meet on or about July 23, 2016, at an elementary school located in Lancaster, Pennsylvania and that

BLEIER drove her to a business parking lot in Lancaster, Pennsylvania where BLEIER performed oral sex on Minor #1 as well as digitally penetrated Minor #1 with his finger.

10. On January 23, 2019, BLEIER gave a post-Mirandized statement to the FBI. Among other things, BLEIER admitted to having an online relationship with Minor #1 and having conversations that were sexual in nature. BLEIER also admitted to communicating with Minor #1 and exchanging pictures that were sexual in nature with Minor #1 via “KIK” and other platforms. BLEIER further admitted knowing Minor #1 was under the age of 18 and further admitted to traveling from Rochester New York to Lancaster Pennsylvania to meet Minor #1. BLEIER further admitted engaging in oral sex with Minor #1 and inserting his finger into MINOR #1’s vagina when he met her in Lancaster, Pennsylvania.

11. Your affiant is advised by FBI Task Officer (“TFO”) Randall Zook he obtained a court order from KIK Interactive for subscriber information for a user “nyhockeyguy09,” a KIK account which is linked to BLEIER. TFO Zook obtained subscriber information listing the user’s first name as “:smile:All” and the user’s last name as “Hers:smile”. These results also list the device type as “Samsung” and the model as “SAMSUNG-SM-G935A,” which is the same model cellular phone as the SUBJECT PROPERTY. These records match the screen shot of BLEIER’s KIK account that MINOR #1 provided to TFO Zook. Minor #1 advised FBI she communicated with Bleier via KIK on this account.

12. KIK Messenger, commonly called KIK, is a proprietary instant messenger software application (app) for mobile devices from the Canadian company KIK Interactive, available free of charge on iOS, Android, and Windows Phone operating systems. KIK uses a smartphones data plan or Wi-Fi to transmit and receive messages, photos, videos, sketches, mobile webpages, and other content after users register a username. Although KIK is designed

to be a mobile application, there are common place methods to install and use KIK on personal computers.

13. The SUBJECT PROPERTY was recovered from BLEIER's person during his arrest on January 23, 2019. During BLEIER's post- Mirandized statement to the FBI he disclosed he had the SUBJECT PROPERTY for approximately three to four years. BLEIER advised the FBI that he may have had the SUBJECT PROPERTY during the timeframe he traveled to Lancaster, Pennsylvania to meet Minor #1 but wasn't sure. BLEIER advised FBI special agents that he had another phone prior to having the SUBJECT PROPERTY and obtained the SUBJECT PROPERTY when his old phone was damaged. BLEIER advised FBI special agents that he was not certain of the exact date he broke the old phone but believed it was late in the year 2016 or early in the year 2017. BLEIER stated he used the same Google account and believes his Google photos, Google drive, and anything else that is backed up to his Google account would be on the SUBJECT PROPERTY. BLEIER told FBI agents he believes some of the old phone numbers may have also transferred to the new phone. BLEIER confirmed to FBI that his old phone was serviced by Verizon Wireless and had number 585-944-8091. BLEIR further confirmed the SUBJECT PROPERTY was serviced through AT&T and had number 585-413-7886.

14. TFO Zook advised your affiant that he obtained Verizon Wireless records for cellular number 585-944-8091 which confirmed that number was in use by another individual from 2014 to October 2016. Based on the fact that BLEIER admitted to switching cellular phones at the time his old phone was damaged and the old number BLEIER had was owned by another individual during the timeframe BLEIER was communicating with Minor #1 and traveled to meet Minor #1, TFO Zook has probable cause to believe BLEIER may have had and

used the SUBJECT PROPERTY during the time he enticed Minor 1 and traveled to engage in sexual contact with Minor 1.

15. The SUBJECT PROPERTY is currently secured at the Lancaster Police Station located at 39 West Chester Street, Lancaster, Pennsylvania and has been there since its recovery from BLEIER during his arrest. In my training and experience, I know that the SUBJECT PROPERTY has been stored in a manner in which its contents are in substantially the same state as it was when the SUBJECT PROPERTY first came into the possession of the FBI and Lancaster Police.

USE OF CELLULAR PHONES IN THE ENTRICEMENT OF MINORS

16. Based on my training and experience, I know that a cellular telephone (or mobile telephone, or wireless telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A cellular telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Cellular telephones may also include global positioning system ("GPS") technology for determining the location of the device.

17. Based on my training, experience, and consultation with other law enforcement officers, I have learned that individuals involved in using an interstate commerce facility to entice a minor to engage in sexually explicit conduct and who travel with the intent to engage in illicit sexual conduct use cellular telephones and maintain these phones on their person. Individuals involved in using an interstate commerce facility to entice a minor to engage in sexually explicit conduct and who travel with the intent to engage in illicit sexual conduct use cellular telephones to communicate with minors, exchange sexually explicit messages with minors and share sexually explicit photographs with minors. Individuals also use cellular telephones to convince minors to take and send sexually explicit photographs of themselves. Cell phones contain wire and electronic data concerning telephonic contact records, text messages, and electronic mail messages. Individuals involved in illicit commercial sex utilize cellular telephones to take photographs and videos of themselves as well as receive photographs and videos of the minors they encounter. Individuals who utilize cell phones to entice a minor to engage in sexually explicit conduct and who travel with the intent to engage in illicit sexual conduct often maintain photos, either taken with the camera function of that particular phone, or digitally transferred from a previously owned phone, of current and/or prior victims for extended periods of time for the purpose of reusing the photographs for their sexual gratification. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

18. From my training and experience, I know that a cellular telephone such as the SUBJECT PROPERTY typically contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to the call log, a cellular telephone such as the SUBJECT PROPERTY typically has the ability to store names and phone

numbers in electronic “address books”; to send, receive, and store text messages and/or e-mail; to take, send, receive, and store photographs and/or video; to store and play back audio files; to store dates, appointments, and other information on personal calendars; and to access websites and download information from the Internet. Photos taken with the camera would remain on the camera until deleted. The phone would also keep Internet history files that would show websites that the phone visited. Moreover, I am aware that the above-described information, once stored digitally on a device such as the SUBJECT PROPERTY, typically remains on the device for long periods of time and is not removed unless actively deleted by a user (and may, in fact, remain on the device even if marked for deletion by a user). Because phones use flash memory, the data will not be retained as long as on the typical hard drive on a computer, but it can still remain for periods of time even after a user deletes it

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

19. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, items that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

20. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the SUBJECT PROPERTY was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the SUBJECT PROPERTY because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

21. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the SUBJECT PROPERTY consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

22. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement’s possession, the execution of this warrant does not involve

the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

23. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the items described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



DARON SCHREIER
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on 11/12, 2019



HONORABLE LYNNE A. SITARSKI
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

One cellular phone, manufactured by Samsung, Model: SM-G935A, Serial Number: RF8HB3BTYND, currently located in secure holding within the Lancaster Police Station, 39 West Chester, Lancaster, Pennsylvania.

This warrant authorizes the forensic examination of the SUBJECT PROPERTY for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the SUBJECT PROPERTY described in Attachment A that relate to violations of 18 U.S.C. § 2422 (Enticement of a minor to engage in sexual conduct) and 18 U.S.C. §2423 (Travel with intent to engage in illicit sexual conduct) including:
 - a. records and information relating to any attempt to persuade, entice, induce or coerce of any individual to manufacture, produce, send and/or receive images or video depicting child pornography and/or sexual exploitation of children under the age of 18;
 - b. call logs demonstrating incoming or outgoing telephone calls between the SUBJECT PROPERTY and other telephone numbers, including the date and time of such telephone call relating to the enticement of a minor to engage in sexual conduct and travel with the intent to engage in illicit sexual conduct;
 - c. text messages or other electronic messages regarding the enticement of a minor to engage in sexual conduct and travel with the intent to engage in illicit sexual conduct;
 - d. any photographs of minors or individuals involved in sex conduct;
 - e. contact lists and electronic address books tending to establish the identity of persons in contact with the SUBJECT PROPERTY;
 - f. evidence of the historical location of the SUBJECT PROPERTY, to the extent contained within the SUBJECT PROPERTY itself;

- g. content of messages, installed applications;
- h. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- i. records and information relating to any travel across state lines to meet the victim and engage in any illegal sexual activity;
- j. records and information relating to the transportation across state lines of any individuals with the intent that they engage in illegal sexual activity.

2. Evidence of user attribution showing who used or owned the SUBJECT PROPERTY at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

3. For the cellular telephones or storage media (including data storage on a cellular telephone) whose seizure is otherwise authorized by this warrant, and the cellular telephones or storage media that contain or in which is stored records or information that is otherwise called for by this warrant:

- a. evidence of who used, owned, or controlled the cellular telephone at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the cellular telephone, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the cellular telephone was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the cellular telephone user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the cellular telephone of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the cellular telephone;
- h. evidence of the times the cellular telephone was used;

- i. passwords, encryption keys, and other access devices that may be necessary to access the cellular telephone ;
- j. documentation and manuals that may be necessary to access the cellular telephone or to conduct a forensic examination of the cellular telephone;
- k. records of or information about Internet Protocol addresses used by the cellular telephone ;
- l. records of or information about the cellular telephone's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. records of or information about the cellular telephones location, including any applications used to map trips or provide step by step directions on any trips taken.
- n. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.